Claims

What is claimed is:

1. A network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system operably coupled with a host bus in the host system, the bus interface system being adapted to transfer data between the network interface system and the host system;

a media access control system operably coupled with the network, the media access control system being adapted to transfer data between the network interface system and the network;

a security system adapted to selectively encrypt outgoing data and to selectively decrypt incoming data from the network; and

a memory system, comprising first and second memories, the first memory being coupled with the media access control system and the security system and storing data from the network prior to security processing, the second memory being coupled to the security system and the bus interface system and storing data processed by the security system prior to transfer to the host system;

wherein the security system comprises an input control system that controls data flow from the first memory into the security processing system, a core module that performs security processing on data received from the input control system, and an output control system that controls data flow from the security system to the second memory system; and

wherein the security system is configured to allow out-of-order writing of packet data to the output control system and the output control system assembles the out-of-order data in correct order within the second memory.

2. The network interface system of claim 1, wherein the bus interface system, the media access control system, the memory system, and the security system are included within a single integrated circuit.

3. The network interface system of claim 1, wherein the input control system writes control words or status words associated with packets to be processed directly to the output control system, bypassing the core module.

4. The network interface system of claim 1, wherein the output control system is configured to receive one or more status words for a packet prior to its payload.

5. The network interface system of claim 1, wherein the output control system is configured to receive control words for a packet while still waiting for part of a preceding packet.

6. The network interface system of claim 5, wherein the part of the preceding packet comprises processed payload data within the core module.

7. The network interface system of claim 1, wherein the output control system is configured to receive one or more status words for a packet after receiving part of a subsequent packet.

8. The network interface system of claim 1, wherein the control module is configured to write decrypted data for a current packet prior to the second memory to writing a status word for a preceding packet thereto.

9. The network interface system of claim 1, wherein the input control system is configured to selectively provide one copy of an initialization vector to the core module and another copy directly to the output control system.

10. The network interface system of claim 1, wherein:

the second memory is not word-addressable;

the output control system comprises a word addressable buffer; and

the output control system writes the contents of the word addressable buffer to the output buffer.

11. The network interface system of claim 1, wherein the core module selectively authenticates packet using the HMAC-MD5-96 algorithm.

12. The network interface system of claim 1, wherein the core module selectively authenticates packets using the HMAC-SHA-1-96 algorithm.

13. A network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system operably coupled with a host bus in the host system, the bus interface system being adapted to transfer data between the network interface system and the host system;

a media access control system operably coupled with the network, the media access control system being adapted to transfer data between the network interface system and the network;

a security system adapted to selectively decrypt and authenticate incoming data from the network; and

a memory system, comprising first and second memories, the first memory being coupled with the media access control system and the security system and storing data from the network prior to security processing, the second memory being coupled to the security system and the bus interface system and storing data processed by the security system prior to transfer to the host system;

wherein the security system is configured to begin writing decrypted data for a subsequent packet to the second memory while completing authentication for a current packet.

14. The network interface system of claim 13, wherein the bus interface system, the media access control system, the memory system, and the security system are included within a single integrated circuit.

15. The network interface system of claim 13, wherein the security system contains pipelines for authentication and decryption that operate in parallel.

16. The network interface system of claim 13, wherein the core module is operable to decrypt completely the subsequent packet prior to authenticating the current packet.

17. The network interface system of claim 13, wherein the core module authenticates the current packet using the HMAC-MD5-96 algorithm.

18. The network interface system of claim 13, wherein the core module authenticates the current packet using the HMAC-SHA-1-96 algorithm.

19. The network interface system of claim 13, wherein the security system comprises:

an input control system;

a core module coupled to the input control system; and

an output control system coupled to both the input control system and the core module,

wherein the input control system is operable to receive a packet containing a control word data portion, a payload data portion, and a status word data portion, forward the control word data portion and the status word data portion directly to the

output control system, and forward the payload data portion to the core module for decryption and authentication thereof.

20. The network interface system of claim 19, wherein the output control system is operable to write decrypted data for the subsequent packet to the second memory concurrently with the core module completing authentication for the current packet.

21. The network interface system of claim 19, wherein the output control system is operable to transmit the control word data portion, the payload data portion, and the status word data portion of packets to the second memory such that such packet portions are ordered in a predetermined fashion independent of an order such portions are received by the output control system.